UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
NORTHERN DIVISION

ALARIE BOWERMAN, individually and on behalf of those similarly situated, Plaintiff, v. **WALSWORTH PUBLISHING COMPANY, INC.,** Defendants.	Case No. 24-104 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Alarie Bowerman ("Plaintiff") brings this Class Action Complaint ("Complaint"), on behalf of herself and all others similarly situated, against Defendant Walsworth Publishing Company, Inc. ("Walsworth" or "Defendant") for failure to properly secure and safeguard Plaintiff's and Class Members' protected personally identifiable information ("PII") stored within Defendant's information network and alleging as follows, based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which is based on personal knowledge:

NATURE OF THE CASE

1. Entities that provide services in the publishing industry and handle customers' sensitive PII owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of the consumers' PII to unauthorized people, especially hackers with nefarious intentions, will result in harm to the affected individuals, including, but not limited to, the invasion of their private financial matters.

2. The harm resulting from a breach of private data manifests in several ways, including identity theft and financial fraud. The exposure of a person's PII through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and to take several additional prophylactic measures.

3. As a publisher, Walsworth knowingly obtains sensitive consumer PII and has a resulting duty to securely maintain such information in confidence.

4. As discussed in more detail below, Walsworth breached its duty to protect the sensitive PII entrusted to it. As such, Plaintiff brings this Class action on behalf of herself and the thousands of other consumers whose PII was accessed and exposed to unauthorized third parties during a data breach of Defendant's system on December 26, 2023, which Walsworth announced on or about November 22, 2024 (the "Data Breach").

5. Indeed, Walsworth did not inform Plaintiff of the Data Breach until November 22, 2024, even though it became aware of the data breach on or about February 9, 2024.

6. Based on the public statements of Walsworth to date, a wide variety of PII was implicated in the breach, including but not limited to, names, payment card number, expiration date and CVV or security code.

7. As a direct and proximate result of Walsworth's inadequate data security, and its breach of its duty to handle PII with reasonable care, Plaintiff's PII has been accessed by hackers, posted on the dark web, and exposed to an untold number of unauthorized individuals.

8. Plaintiff is now at a significantly increased and certainly impending risk of fraud,

identity theft, and similar forms of criminal mischief, and such risk may last for the rest of her life. Consequently, Plaintiff must devote substantially more time, money, and energy to protect herself, to the extent possible, from these crimes.

9. Plaintiff, on behalf of herself and others similarly situated, brings claims for negligence, negligence *per se*, breach of fiduciary duty, and unjust enrichment, seeking actual and putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

10. To recover from Walsworth for her sustained, ongoing, and future harms, Plaintiff seeks damages in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring Defendant to: 1) disclose, expeditiously, the full nature of the Data Breach and the types of PII accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of PII possessed by Defendant; and 3) provide, at its own expense, all impacted victims with lifetime identity theft protection services.

PARTIES

Plaintiff

11. Plaintiff Alarie Bowerman is an adult individual and, at all relevant times herein, a resident and citizen of Arkansas, residing in Bella Vista, Arkansas. Plaintiff is a victim of the Data Breach.

12. Plaintiff is a customer of Defendant and her information was stored with and handled by Defendant as a result of her dealings with Defendant.

13. On or about November 22, 2024, Plaintiff was notified of the Data Breach and of the impact to her PII via letter from Walsworth.

14. As a result of Defendant's conduct, Plaintiff suffered actual damages including, without limitation, time related to monitoring her financial accounts for fraudulent activity, facing

an increased and imminent risk of fraud and identity theft, the lost value of her personal information, and other economic and non-economic harm. Plaintiff and Class members will now be forced to expend additional time, efforts, and potentially expenses to review their credit reports, monitor their financial accounts, and monitor for fraud or identify theft.

Defendant Walsworth Publishing Company, Inc.

15. Defendant Walsworth Publishing Company, Inc., is a Missouri corporation with its principal place of business at 306 N. Kansas Avenue, Marceline, Missouri 64658.

16. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Plaintiff.

17. Plaintiff will seek leave of court to amend this Complaint to reflect the true names and capacities of the responsible parties when their identities become known.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d). The amount in controversy in this Class action exceeds $5,000,000, exclusive of interest and costs, and there are numerous Class members who are citizens of states other than Defendants' state of citizenship.

19. This Court has personal jurisdiction over the parties in this case. Defendant conducts business in this District and is a citizen of this District by virtue of having its principal place of business located in this District.

20. Venue is proper in this District under 28 U.S.C. §1391(b) because Walsworth and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL BACKGROUND

A. Walsworth Publishing Company, Inc. and the Services it Provides.

21. Founded in 1937, Walsworth is a family owned printing company that produces books, catalogs and magazines.

22. For its customers, Walsworth receives and handles PII, which includes, *inter alia*, consumers' full name and payment information.

23. To purchase items from Walsworth, consumers are required to entrust their highly sensitive PII to Defendant. Plaintiff entrusted this information to Walsworth with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

24. By obtaining, collecting, and storing Plaintiff's PII, Walsworth assumed legal and equitable duties and knew or should have known that Defendant was responsible for protecting Plaintiff's PII from unauthorized disclosure.

25. And, upon information and belief, Defendant funds its data security measures entirely from its general revenue, including services provided by or on behalf of Plaintiff and the Class members.

B. Walsworth Publishing Company, Inc. Knew the Risks of Storing Valuable PII and the Foreseeable Harm to its Customers.

26. At all relevant times, Walsworth knew it was storing sensitive PII and that, as a result, its systems would be an attractive target for cybercriminals.

27. Walsworth also knew that a breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised.

28. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As

one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[1]

29. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[2]

30. The type and breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendants' patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

31. PII is a valuable property right.[3] The value of PII as a commodity is measurable.[4] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[5] American companies are estimated to have spent over $19 billion on acquiring

[1] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[2] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Apr. 17, 2023).

[3] *See* Marc Van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION & COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . . ").

[4] Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle. /824192.

[5] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

personal data of consumers in 2018.[6] It is so valuable to identity thieves that once PHI/PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

32. As a result of their real value and the recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated, and become more valuable to thieves and more damaging to victims.

33. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[7]

34. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will

[6] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[7] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 17, 2023).

be deceived into providing the criminal with additional information.

35. Consumers and employees place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[8]

36. Given these facts, any company that has customers and then compromises the privacy of customers' PII has thus deprived that customer of the full monetary value of the customers' purchase from the company.

37. Based on the value of its customers' PII to cybercriminals and cybercriminals', Walsworth certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

C. Walsworth Publishing Company, Inc. Breached its Duty to Protect its Customers' PII.

38. On November 22, 2024 Walsworth announced that it experienced a security incident disrupting access to its systems.

39. As noted above, the customer PII compromised in the Data Breach includes employee names and financial account and/or payment information.

40. Like Plaintiff, other potential Class members received similar notices informing them that their PII was exposed in the Data Breach.

41. All in all, tens of thousands of individuals with information stored on Walsworth's

[8] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) Information Systems Research 254 (June 2011), https://www.guanotronic.com/~serge/papers/weis07.pdf.

system had their PII breached.

42. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures to protect its employees' PII.

D. FTC Guidelines Prohibit Walsworth Publishing Company, Inc. from Engaging in Unfair or Deceptive Acts or Practices.

43. Walsworth is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

44. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[9]

45. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[10]

46. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor suspicious activity on the network; and verify that third-party service providers have implemented reasonable security

[9] *Start with Security – A Guide for Business*, United States Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[10] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformation.pdf.

measures.[11]

47. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

48. Walsworth failed to properly implement basic data security practices. Walsworth's failure to employ reasonable and appropriate measures to protect against unauthorized access to its customers' PII constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

49. Walsworth was at all times fully aware of its obligations to protect customers' PII of because of its position as a publisher, which gave it direct access to reams of customer PII. Defendant is also aware of the significant repercussions that would result from its failure to do so.

E. Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft.

50. Cyberattacks and data breaches at companies like Walsworth are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

51. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[12]

52. That is because any victim of a data breach is exposed to serious ramifications

[11] *Id.*

[12] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007), https://www.gao.gov/new.items/d07737.pdf.

regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and to take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

53. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to exhaust financial accounts, receive medical treatment, open new utility accounts, and incur charges and credit in a person's name.

54. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing freezes on their credit, and correcting their credit reports.[13]

55. Identity thieves use stolen personal information for a variety of crimes, including

[13] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last accessed Feb. 24, 2023).

credit card fraud, phone or utilities fraud, and bank/finance fraud. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.

56. Identity thieves can also use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, and/or rent a house or receive medical services in the victim's name.

57. Moreover, theft of PII is also gravely serious because PII is an extremely valuable property right.[14]

58. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves.

59. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States. For example, with the PII stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file

[14] *See, e.g.*, John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiff.

60. As discussed above, PII is such a valuable commodity to identity thieves, and once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

61. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against companies like Walsworth is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

62. Indeed, a Social Security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[15] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[16]

63. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to PII, they *will use it.*[17]

---

[15] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

[16] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[17] *Id.*

64. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years later. As with income tax returns, an individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notified the individual's employer of the suspected fraud.

65. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[18]

66. Cybercriminals can post stolen PII on the cyber black market for years following a data breach, thereby making such information publicly available.

67. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it happened. [19] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[20]

68. Identity theft victims must spend countless hours and large amounts of money

[18] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

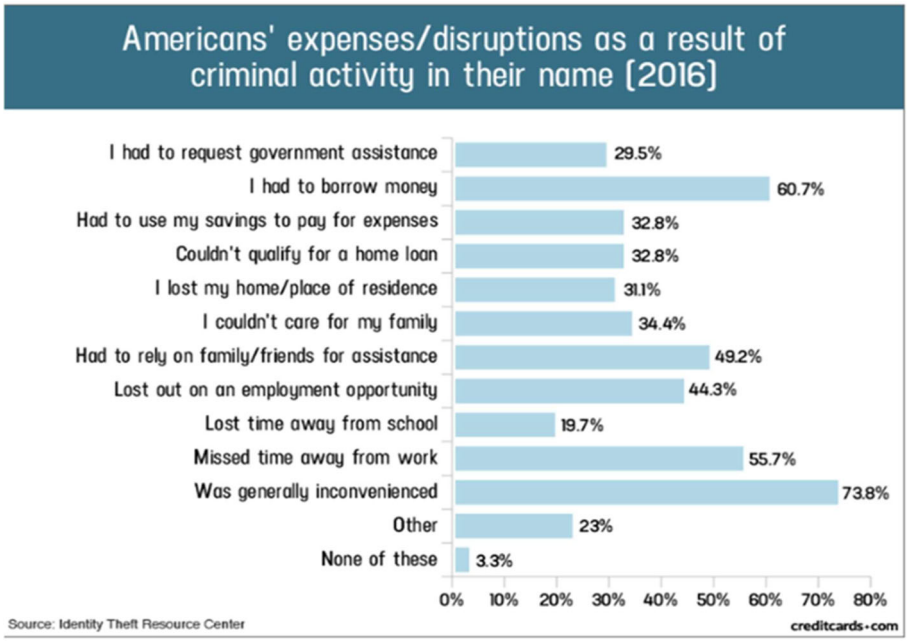
[19] *See* Medical ID Theft Checklist, https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last visited Apr. 17, 2023).

[20] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages")*, EXPERIAN, https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited Apr. 17, 2023).

repairing the impact to their credit as well as protecting themselves in the future.[21]

69. It is within this context that Plaintiff must now live with the knowledge that her PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

70. A study by the Identity Theft Resource Center shows the multitude of harm caused by fraudulent use of personal and financial information.



71. Victims of the Data Breach, like Plaintiff, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[22]

72. As a direct and proximate result of the Data Breach, Plaintiff has had her PII exposed, has suffered harm as a result, and have been placed at an imminent, immediate, and

[21] *Guide for Assisting Identity Theft Victims*, FED. TRADE COMM'N, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

[22] *Id.*

continuing increased risk of harm from fraud and identity theft. Plaintiff must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on her everyday life, including purchasing identity theft and credit monitoring services every year for the rest of her life, placing "freezes" and "alerts" with credit reporting agencies, contacting her financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

73. Moreover, Plaintiff and Class members have an interest in ensuring that their PII, which remains in the possession of Walsworth, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Walsworth has shown itself to be wholly incapable of protecting Plaintiff's PII.

74. Plaintiff and Class members also have an interest in ensuring that their personal information that was provided to Walsworth is removed from Walsworth's unencrypted files.

F. Plaintiff Suffered Damages.

75. Walsworth received Plaintiff's and class members' PII in connection with their purchasing products from Walsworth. In requesting and maintaining Plaintiff's PII for business purposes, Walsworth expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff's and Class members' PII. Walsworth did not, however, take proper care of Plaintiff's and Class members' PII, leading to its exposure to and exfiltration by cybercriminals as a direct result of Walsworth's inadequate security measures.

76. For the reasons mentioned above, Walsworth's conduct, which allowed the Data Breach to occur, caused Plaintiff and Class members significant injuries and harm in several ways. Plaintiff and Class members must immediately devote time, energy, and money to: 1) closely

monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them. Plaintiff and Class members have taken or will be forced to take these measures to mitigate their potential damages as a result of the Data Breach.

77. Once PII is exposed, there is little that can be done to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class members will need to maintain these heightened measures for years, and possibly their entire lives because of Defendant's conduct.

78. Further, the value of Plaintiff's and Class members' PII has been diminished by its exposure in the Data Breach. Plaintiff and Class members were damaged in an amount at least equal to the difference in the value between the services they thought they provided (which would have included adequate data security protection) and the payments they actually received.

79. Plaintiff and Class members would not have made purchases from Walsworth, had they known that Walsworth would negligently fail to adequately protect their PII. Indeed, Plaintiff and Class members psid for goods with the expectation that Walsworth would keep their PII secure and inaccessible from unauthorized parties. Plaintiff and Class Members would not have purchased goods from Walsworth had they known that Defendant failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their PII from criminal theft and misuse.

80. As a result of Defendants' failures, Plaintiff and Class Members are also at

substantial and certainly impending increased risk of suffering identity theft and fraud or misuse of their PII.

81. Further, because Defendant delayed in notifying Plaintiff about the Data Breach for nearly eleven months, Plaintiff was unable to take affirmative steps during that time period to attempt to mitigate any harm or take prophylactic steps to protect against injury.

82. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[23]

83. Plaintiff is also at a continued risk because their information remains in Walsworth' computer systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Walsworth fails to undertake the necessary and appropriate security and training measures to protect its customers' PII.

84. In addition, Plaintiff and Class members have suffered emotional distress because of the Data Breach, and the increased risk of identity theft and financial fraud.

CLASS ALLEGATIONS

85. Plaintiff brings all counts, as set forth below, individually and as a Class action, pursuant to the provisions of the Fed. R. Civ. P. 23, on behalf of a Class defined as:

> All individuals within the United States whose PII was accessed in the Data Breach (the "Class").

86. Excluded from the Class is Defendant, its subsidiaries and affiliates, officers and

[23] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KNOWBE4, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited Apr. 17, 2023).

directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

87. This proposed Class definition is based on the information available to Plaintiff currently. Plaintiff may modify the Class definition in an amended pleading or when she moves for Class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

88. **Numerosity – Fed. R. Civ. P. 23(a)(1)**: Plaintiff is informed and believes, and thereon alleges, that there are at minimum 107,707 of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Walsworth's records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes at least 107,707 individuals.

89. **Commonality – Fed. R. Civ. P. 23(a)(2):** This action involves questions of law and fact common to the Class. Such common questions include, but are not limited to:

a. Whether Walsworth failed to timely notify Plaintiff of the Data Breach;

b. Whether Walsworth had a duty to protect Plaintiff's and Class Members' PII;

c. Whether Walsworth was negligent in collecting and storing Plaintiff's and Class Members' PII, and breached its duties thereby;

d. Whether Defendant breached its fiduciary duty to Plaintiff and the Class;

e. Whether Walsworth was unjustly enriched;

f. Whether Plaintiff and Class members are entitled to damages because of Walsworth's wrongful conduct; and

g. Whether Plaintiff and Class members are entitled to restitution because of Walsworth's wrongful conduct.

90. **Typicality – Fed. R. Civ. P. 23(a)(3)**: Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and members of the Class all had information stored in Walsworth's System, each having their PII exposed and/or accessed by an unauthorized third party.

91. **Adequacy of Representation – Fed. R. Civ. P. 23(a)(3)**: Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the other Class members Plaintiff seeks to represent; Plaintiff has retained counsel competent and experienced in complex Class action litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel have adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

92. **Injunctive Relief, Fed. R. Civ. P. 23(b)(2):** Defendant has acted and/or refused to act on grounds that apply generally to the Class therefore making injunctive and/or declarative relief appropriate with respect to the Class under 23(b)(2).

93. **Superiority, Fed. R. Civ. P. 23(b)(3):** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying

adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Walsworth. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

94. Walsworth has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

95. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Walsworth failed to timely and adequately notify the public of the Data Breach;

b. Whether Walsworth owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Walsworth's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Walsworth's failure to institute adequate protective security measures amounted to negligence;

e. Whether Walsworth failed to take commercially reasonable steps to safeguard employee PII; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

96. Finally, all members of the proposed Class are readily ascertainable. Walsworth has access to Class members' names and addresses affected by the Data Breach. Class members have already been preliminarily identified and sent notice of the Data Breach by Walsworth.

FIRST CAUSE OF ACTION
NEGLIGENCE
(Plaintiff on behalf of the Class)

97. Plaintiff restates and reallege the preceding allegations above as if fully alleged herein.

98. Plaintiff brings this claim individually and on behalf of the Class.

99. Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, and control.

100. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

101. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendant. By collecting and storing valuable PII that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

102. Defendant's duty also arose from Defendant's position as a publisher which transacted directly with consumers. Defendant assumes a duty to reasonably protect consumers' information.

103. Defendant breached the duties owed to Plaintiff and Class Members and thus were negligent. As a result of a successful attack directed towards Defendant that compromised Plaintiff's and Class members' PII, Defendant breached its duties through some combination of

the following errors and omissions that allowed the data compromise to occur:

(a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of employee information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; and (g) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII.

104. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised.

105. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered injuries, including, but not limited to:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff' and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

106. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in

an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE
(Plaintiff on behalf of the Class)

107. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

108. Plaintiff brings this claim individually and on behalf of the Class.

109. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendant for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

110. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach involving PII of its employees.

111. Plaintiff and members of the Class are consumers within the Class of persons Section 5 of the FTC Act was intended to protect.

112. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

113. The harm that has occurred because of Defendant's conduct is the type of harm that the FTC Act and Part 2 was intended to guard against.

114. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY

(Plaintiff on behalf of the Class)

115. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

116. Plaintiff and Class Members have an interest, both equitable and legal, in the PII about them that was conveyed to, collected by, and maintained by Defendant and that was ultimately accessed or compromised in the Data Breach.

117. As a business, and recipient of consumers' PII, Defendant has a fiduciary relationship to its consumers, including Plaintiff and the Class members.

118. Because of that fiduciary relationship, Defendant was provided with and stored private and valuable PII related to Plaintiff and the Class. Plaintiff and the Class were entitled to expect their information would remain confidential while in Defendant's possession.

119. Defendant owed a fiduciary duty under common law to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

120. As a result of the parties' fiduciary relationship, Defendant had an obligation to maintain the confidentiality of the information within Plaintiff's and the Class Members' PII.

121. Defendant's customers, including Plaintiff and Class members, have a privacy interest in personal financial matters, and Walsworth had a fiduciary duty not to disclose personal data concerning its customers.

122. As a result of the parties' relationship, Defendant had possession and knowledge of confidential PII of Plaintiff and Class Members, information not generally known.

123. Plaintiff and Class members did not consent to nor authorize Defendant to release

or disclose their PII to unknown criminal actors.

124. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by, among other things:

a. mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII;

b. mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks;

c. failing to design and implement information safeguards to control these risks;

d. failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures;

e. failing to evaluate and adjust its information security program in light of the circumstances alleged herein;

f. failing to detect the breach at the time it began or within a reasonable time thereafter; and

g. failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive PII.

125. But for Defendant's wrongful breach of its fiduciary duties owed to Plaintiff and Class Members, their PII would not have been compromised.

126. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered injuries, including:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fail to undertake appropriate and adequate measures to protect

Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

127. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(Plaintiff on behalf of the Class)

128. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

129. Upon information and belief, Defendant funds its data security measures entirely from its general revenue provided by or on behalf of Plaintiff and the Class members.

130. As such, a portion of the revenue provided by or on behalf of Plaintiff's and the Class Members is to be used to provide a reasonable level of data security.

131. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided monetary payments to Defendant and in so doing provided Defendant with their PII. In exchange, Plaintiff and Class Members should have received from Defendant the goods that were the subject of the relationship and have their PII protected with adequate data security.

132. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff's and

Class members for business purposes.

133. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

134. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by its common law and statutory duties.

135. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiff's and Class Members provided.

136. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

137. If Plaintiff and Class Members knew that Defendant had not reasonably secured their PII, they would not have agreed to provide their PII to Defendant.

138. Plaintiff and Class Members have no adequate remedy at law.

139. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered injuries, including, but not limited to:

a. Theft of their PII;

b. Costs associated with purchasing credit monitoring and identity theft

protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who

likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

140. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

141. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, pray for relief as follows:

a. For an Order certifying this action as a Class action and appointing Plaintiff as a Class Representative and her counsel as Class Counsel;

b. For equitable relief enjoining Walsworth from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;

c. For equitable relief compelling Walsworth to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Personal Information compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Walsworth's wrongful conduct;

e. Ordering Walsworth to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g. For an award of punitive damages, as allowable by law;

h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i. Pre- and post-judgment interest on any amounts awarded; and,

j. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded by Plaintiff on all claims so triable.

Dated: December 12, 2024

Respectfully submitted,

/s/James J. Rosemergy

CAREY DANIS & LOWE
James J. Rosemergy #111477
8235 Forsyth Blvd., Suite 1100
Clayton, MO 63105
Tel.: 314-725-7700
Fax: 314-721-0905
jrosemergy@careydanis.com

Marc H. Edelson (*pro hac vice* forthcoming)
EDELSON LECHTZIN LLP
411 S. State Street, Suite N300
Newtown, PA 18940
T: (215) 867-2399
medelson@edelson-law.com

Attorneys for Plaintiff and the Putative Class